Analisa *Network Forensics* Pada Serangan *Botnet*

[1] Yonathan Satrio Nugroho, [2] Irwan Sembiring
Fakultas Teknologi Informasi
Universitas Kristen Satya Wacana
Jl. Diponegoro 52-60, Salatiga 50771, Indonesia
Email: [1] 672012193@student.uksw.edu, [2] irwan@staff.uksw.edu

Abstract

Nowadays the internet users manipulated with several web applications which instruct them to download and install in order to pc's system stabilities or other aims. Well, most of users don't realize the applications might have been added with some malicious software such as Worms, and Trojan horse. After the malware infects the victim's computer, it makes them as slave as they dedicate machine to the master's purposes, and it known as botnet. Botnet is categorized as difficult detected malvare even with up-to-date antivirus software and causing lot of problems. Network Security Researcher has developed various methods to detect Botnet invasion, one of the method is using forensics method. Network forensics is a branch of Digital forensics which the main task is to analyze the problem (e.g Botnet's attack) by identify, classify the networks traffic and also recognize the attacker's behavior in network. The output of this system will produce the pattern recognition of Botnet's attack and payload identification according to Network Forensics Analysis.

***Keywords** : Malware, Botnet, Network Forensics*

Abstrak

Di masa sekarangm para pengguna internet kadang terkecoh dengan beberapa aplikasi di internet yang menginstruksikan mereka untuk mengunduh dan memasang aplikasi tersebut. Tanpa berpikir panjang, banyak pengguna mengikuti instruksi tersebut dan tidak menyadari bahwa aplikasi yang mereka pasang (*install*) telah disisipi dengan *software* berbahaya seperti *Worms*, dan *Trojan horse*. Setelah malware tersebut terpasang dan menginfeksi komputer korban, komputer korban berubah menjadi mesin yang bekerja di bawah arahan pengendalinya, mesin tersebut disebut sebagai *botnet*. *Botnet* dikelompokkan sebagai *malicious software* (*malware*) yang susah dilacak bahkan dengan menggunakan antivirus yang terbaru. Salah satu metode untuk mendeteksi serangan *botnet* adalah dengan metode forensik. Forensik jaringan merupakan salah satu ilmu cabang dari Forensik digital, dimana salah satu tugas utamanya adalah menganalisa masalah seperti serangan *Botnet* dengan mengidentifikasi dan mengklasifikasi *networks traffic*, serta mengidentifikasi kecenderungan pola serang *attacker* pada jaringan. Penelitian ini menghasilkan identifikasi pola serangan *Botnet* dan identifikasi *payload* berdasar pada analisa Forensik Jaringan.

Kata Kunci : *Malware*, *Botnet*, Forensik Jaringan

---

[1] Mahasiswa Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana Salatiga

[2] Staff Pengajar Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana Salatiga